UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

BRENT GARBACK,

Plaintiff,

v.

LINDA LOSSING, MARVIN SHWEDEL, CYBER-TRACE TECHNOLOGIES, and JOHN SAVAGE,

Defendants.
_____/

Case No. 09-cv-12407

HONORABLE STEPHEN J. MURPHY, III

OPINION AND ORDER GRANTING DEFENDANT SHWEDEL'S MOTION TO DISMISS (docket no. 5) **AND GRANTING LEAVE TO FILE AMENDED COMPLAINT**

Plaintiff Brent Garback has sued the above defendants for allegedly hacking into his email account and reading his emails. Information in emails between Garback and his divorce attorney was then allegedly used for the purpose of obtaining an advantage in negotiating a divorce settlement between Garback and his ex-wife, defendant Linda Lossing. Garback alleges violations of Titles I and II of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq*., as well as other state law claims. Defendant Marvin Shwedel moves under Fed. R. Civ. P. 12(b)(6) to dismiss the claims asserted against him. For the reasons below, the Court grants the motion and will give Garback 21 days to file an amended complaint to remedy the various deficiencies cited herein.

FACTS

The following facts are alleged in the complaint. Brent Garback was once married to Defendant Linda Lossing. Compl. ¶ 7. Lossing and Garback divorced in June 2007. *Id.* Defendant Marvin Shwedel represented Lossing in the divorce proceedings. *Id.* ¶ 8. In December 2005, after extensive negotiations, Garback and Lossing reached a settlement

agreement, the details of which are not relevant here. *Id.* ¶ 10. In June 2007, Garback discovered that during the divorce proceedings, Lossing had allegedly conspired with the other defendants for the purpose of intercepting Garback's emails between he and his divorce counsel. Defendants then used the information in the emails to craft negotiating points and ultimately a more favorable divorce settlement. *Id.* ¶ 12.

More specifically, Garback alleges that Lossing, knowing that Garback often communicated with his attorney by email, hired Defendant Cyber-Trace Technologies ("Cyber-Trace") for the purpose of "hacking" into Garback's email accounts to access "stored communications" maintained by Garback's internet service provider ("ISP"). *Id.* ¶ 14. Defendant John Savage directed the services of Cyber-Trace. *Id.* ¶ 15. When Lossing received the emails from Cyber-Trace, she passed them to Shwedel, who used them to gain a negotiating advantage in the divorce proceedings. *Id.* ¶¶ 15, 17.

DISCUSSION

A. Legal Standard - Rule 12(b)(6)

"[W]hen the allegations in a complaint, however true, could not raise a claim of entitlement to relief, 'this basic deficiency should . . . be exposed at the point of minimum expenditure of time and money by the parties and the court.' " *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007) (quoting 5 C. Wright & A. Miller, Federal Practice and Procedure § 1216, pp. 233-34 (3d ed. 2004)). Accordingly, Federal Rule of Civil Procedure 12(b)(6) allows a defendant to test whether, as a matter of law, the plaintiff is entitled to legal relief even if everything alleged in the complaint is true. *See Mayer v. Mylod*, 988 F.2d 635, 638 (6th Cir. 1993).

In assessing a motion brought pursuant to Rule 12(b)(6), the court must presume as true all well-pleaded factual allegations in the complaint and draw all reasonable inferences

from those allegations in favor of the non-moving party. *Bishop v. Lucent Techs., Inc.*, 520 F.3d 516, 519 (6th Cir. 2008). Although the pleading standard is liberal, and the court must accept as true all allegations in the complaint, the court need not accept as true any legal conclusion alleged therein, even if couched as a factual allegation. *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1945 (2009). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.*

The Federal Rules of Civil Procedure do not require a claimant to set out in detail the facts upon which he bases his claim. To the contrary, all the Rules require is "a short and plain statement of the claim" that gives the defendant fair notice of what the plaintiff's claim is and the grounds upon which it rests. Fed. R. Civ. P. 8(a). This requires that a claimant put forth "enough facts to raise a reasonable expectation that discovery will reveal evidence of [the requisite elements of the claim]." *Bell Atl.*, 550 U.S. at 556. Thus, although "a complaint need not contain 'detailed' factual allegations, its '[f]actual allegations must be enough to raise a right to relief above the speculative level on the assumption that all the allegations in the complaint are true.'" *Ass'n of Cleveland Fire Fighters v. Cleveland, Ohio*, 502 F.3d 545, 548 (6th Cir. 2007) (quoting *Bell Atl.*, 550 U.S. at 555). Therefore, the Court will grant a Rule 12(b)(6) motion only in cases where there are simply not "enough facts to state a claim to relief that is plausible on its face." *Bell Atl.*, 550 U.S. at 570. "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged – but it has not 'show[n]' – 'that the pleader is entitled to relief.'" *Iqbal*, 129 S. Ct. at 1950 (quoting Fed. R. Civ. P. 8(a)(2)).

B. Analysis

Schwedel seeks dismissal of all counts against him because, he claims, the allegations fail to state a claim for relief. The Court addresses each count below.

1. Count One - Titles I & II of the Electronic Communications Privacy Act

Count one alleges, inartfully, violations of Titles I *and* II of the Electronic Communications Privacy Act of 1986 ("ECPA"), codified at 18 U.S.C. § 2510 and 18 U.S.C. § 2701, respectively. The Court addresses each claim separately.

a. Title I of the ECPA - 18 U.S.C. § 2510 ("The Wiretap Act")

Garback alleges that Shwedel and others violated Title I of the ECPA, 18 U.S.C. § 2511 ("Wiretap Act"), when they allegedly "hacked" into Garback's email account and read his emails. Section 2511 prohibits, among other things, the "interception" of any wire, oral, or electronic communication, 18 U.S.C. § 2511(1)(a), as well as the intentional use of the contents of any electronic communication with knowledge that the information was obtained through the interception of an electronic communication, 18 U.S.C. § 2511(1)(d). These provisions may be enforced in a civil action brought by one whose communication was intercepted. 18 U.S.C. § 2520(a). Both sides agree that "electronic communication" includes email. The issue here is whether Garback has sufficiently alleged an "interception." Shwedel argues that Garback has failed to allege that *anyone*, let alone Shwedel, "intercepted" Garback's email.

"Intercept" is defined in the Wiretap Act as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The Sixth Circuit has not addressed the issue, but another judge from this District has agreed with the other circuits that have. All agree that the term "intercept" "'encompasses only acquisitions *contemporaneous* with transmission.'" *See Bailey v. Bailey*, No. 07-11672, 2008 WL 324156, at *4 (E.D. Mich.

Feb. 6, 2008) (Cox, J.) (emphasis added) (quoting *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003) and citing *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2001); *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003); and *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107 (3rd Cir. 2003)). Judge Cox noted that the general reasoning behind these decisions is that "based on the statutory definition and distinction between 'wire communication' and 'electronic communication,' the latter of which conspicuously does not include electronic storage, Congress intended for electronic communication in storage to be handled solely by the Stored Communications Act." *Bailey*, 2008 WL 324156, *4. As did Judge Cox, the Court finds this reasoning persuasive and adopts it here.

This standard does not require courts to measure the time between transmission and receipt to determine whether an acquisition was contemporaneous with transmission. Rather, courts must consider the *method* used by alleged violators. In *Steiger*, for example, the Eleventh Circuit held that the conduct at issue did not constitute interception when an anonymous source used a Trojan Horse virus. An anonymous source uploaded a photograph with an embedded Trojan Horse virus to an online news group. Once Steiger downloaded the photograph, the virus permitted the anonymous source to enter Steiger's computer via the internet and locate incriminating evidence. The source later passed the evidence to law enforcement. 318 F.3d at 1041-44. Based on this evidence, Steiger was indicted for violating a series of federal statutes involving the sexual exploitation of minors. He moved to suppress the evidence arguing, in part, that the anonymous source violated the Wiretap Act to obtain the evidence. The panel held there had been no interception by

the source.[1] *Id.* at 1046. It adopted the contemporaneity standard used by the Fifth and Ninth Circuits and held:

> [T]here is nothing to suggest that any of the information provided in the source's emails to [law enforcement] was obtained through contemporaneous acquisition of electronic communications while in flight. Rather, the evidence shows that the source used a Trojan Horse virus that enabled him to access and download information stored on Steiger's personal computer. This conduct, while possibly tortious, does not constitute an interception of electronic communications in violation of the Wiretap Act.

Id. at 1050; *see Bailey*, 2008 WL 324156, *4 (no interception where defendant uploaded to plaintiff's computer a program allowing defendant to learn plaintiff's passwords and later used the program to access plaintiff's electronic communications, citing *Steiger* as analagous).

Similarly, courts have found that simply accessing another's stored email does not constitute interception because it is not done contemporaneously with the transmission of the original email. *See, e.g.*, *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003); *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 980-81 (M.D. Tenn. 2008); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 557-58 (S.D.N.Y. 2008). Indeed, interception of email can occur in only a very narrow range of circumstances. The court in *Steiger* described these circumstances:

> [T]here is only a narrow window during which an E-mail interception may occur – the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.

[1] Although the court's holding on this issue is arguably dicta, its reasoning is persuasive nonetheless.

Steiger, 318 F.3d at 1050 (quoting Jarrod J. White, *E-Mail@Work.com: Employer Monitoring of Employee E-Mail*, 48 Ala. L. Rev. 1079, 1083 (1997)).

Applying these standards, the Court concludes that Garback has failed to state a plausible claim against Schwedel for violation of the Wiretap Act. Shwedel asserts that "there is no allegation that any emails were 'intercepted' contemporaneously with transmission. Instead, the complaint alleges that Lossing had [Cyber-Trace] retrieve **stored** emails that had already been delivered to Garback's email account." Def.'s Br., at 3 (emphasis in original). This is a fair characterization of the allegations in the complaint. For example, paragraph 14(1)[2] alleges that Lossing retained the services of Cyber-Trace for the express purpose of "hacking" into Garback's email accounts to access "stored communications" maintained by Garback's ISP before and after the emails were delivered to Garback. This statement does not allege anything close to a contemporaneous interception. Paragraph 18 alleges that "defendants, and each of them, violated the federal Wiretap Act, 18 USC 2520, which prohibits the intentional and unauthorized interception, use or disclosure of electronic communications." This is a pure legal conclusion not entitled to the assumption of truth. *See Iqbal*, 129 S. Ct. at 1950.

Garback acknowledges these deficiencies, but submits that his inartful pleading does not mean he has failed to state a claim. Pl.'s Br., at 10. He claims the allegations are sufficient to provide notice to the defendants of the claims against them, which is all he needs to do. *Id.* He asserts that discovery may show three possible ways in which defendants may have intercepted his emails. First, it may show that they simply rerouted all email intended for Garbak into a new mailbox accessible to the hacker. Second, it may show the hacker inserted a copy-and-forward command that sent a copy of each email to

[2] There are two paragraphs numbered "14".

the hacker when it was received at the server. Third, it may show that the hacker set up a separate notification trigger such that when an email was received and an arrival notice was sent to Garback, a copy of that notice incorporating at least some of that information was also sent to the hacker. *Id.* at 10-11.

While the Court agrees that these factual scenarios might constitute an interception under the standards articulated above, allegations that support these scenarios appear nowhere in the complaint. Garback is speculating. The only place the word "intercept" is even mentioned in the complaint is in paragraph 18, as part of a conclusory allegation. Statements in a brief are not allegations. The complaint lacks sufficient factual allegations to support a claim for violation of the Wiretap Act. *See Found. for Interior Design Educ. Research v. Savannah Coll. of Art & Design*, 244 F.3d 521, 530 (6th Cir. 2001) ("the price of entry, even to discovery, is for the plaintiff to allege a factual predicate concrete enough to warrant further proceedings, which may be costly and burdensome. Conclusory allegations in a complaint, if they stand alone, are a danger sign that the plaintiff is engaged in a fishing expedition." (quoting *DM Research, Inc. v. Coll. of Am. Pathologists*, 170 F.3d 53, 55 (1st Cir.1999))).

The Court will grant Garback leave to file an amended complaint, consistent with Rule 11, that sufficiently pleads interception. Shwedel raises additional arguments in support of dismissing the Wiretap Act claim against him. The Court address these arguments so that in the event Garback files an amended complaint, Shwedel's arguments will hopefully be mooted by Garback's amendments to the complaint. Failure to remedy the deficiencies, however, will result in dismissal of the claims without further leave to amend.

Shwedel argues that, assuming Garback had properly alleged an interception, there are no allegations that Shwedel himself intercepted any emails. Def.'s Br. p. 3. ("[A]nd

certainly, it doesn't allege that Shwedel intercepted any communications"). Shwedel is correct. The complaint alleges only that "Lossing turned over the stolen emails to Shwedel as her attorney" and the two used the emails to craft negotiating positions. Compl. ¶ 17.[3]

Interception, however, is not the only basis for liability under the Wiretap Act. Specifically, § 2511(1)(d) prohibits the intentional use or endeavor to use the contents of an electronic communication, knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of the Wiretap Act. 18 U.S.C. § 2511(1)(d). Accordingly, although Garback does not allege that Shwedel engaged in the actual interception, Shwedel could be liable if he intentionally used the information knowing it was obtained through an unlawful interception. The problem for Garback, however, is that the complaint contains no allegations that Shwedel used any intercepted information with knowledge that it was unlawfully intercepted.[4] Therefore, the complaint would fail to state a claim against Shwedel even if it properly alleged an interception.

---

[3] The complaint also alleges that "defendants," which would include Shwedel, "violated the federal Wiretap Act, 18 USC 2520," Compl. ¶ 18, but as indicated above, this is a bare legal conclusion not entitled to the presumption of truth.

[4]Though the complaint alleges that Shwedel knew the information was "stolen," *see* Compl. ¶ 17, it fails to allege that Shwedel knew the information was obtained through an interception that violated § 2511(1)(d). The difference is significant. Garback must plead that Shwedel had knowledge or reason to know of the illegality of the interception. *See Williams v. Poulos*, 11 F.3d 271, 284 (1st Cir. 1993) ("Thus, in a civil action, a plaintiff must demonstrate '1) the information used or disclosed came from an intercepted communication, and 2) sufficient facts concerning the circumstances of the interception such that the defendant could, with presumed knowledge of the law, determine that the interception was prohibited in light of [§ 2511(a)].'" (quoting *Thompson v. Dulaney*, 970 F.2d 744, 749 (10th Cir. 1992)); *see also United States v. Wulinger*, 981 F.2d 1497, 1501 (6th Cir. 1992) (knowledge or reason to know that the interception itself violated the Wiretap Act in essential element of § 2511(1)(d) criminal offense).

Garback's final effort to breathe life into his Wiretap Act claim is to assert that his failure to allege that Shwedel himself directly intercepted emails is not fatal because the complaint alleges that Shwedel conspired to intercept emails. Pl.'s Resp. Br., at 12. Garback provides no support for his contention that civil liability under the Wiretap Act exists for those actors other than primary interceptors. There is no textual support in the statute for applying secondary liability for Wiretap Act violations. "Normally federal courts refrain from creating secondary liability that is not specified by statute." *Doe v. GTE Corp.*, 347 F.3d 655, 658-59 (7th Cir. 2003) (Easterbrook, J.) (citing *Central Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164 (1994)). "Although a statute's structure may show that secondary liability has been established implicitly," Judge Easterbrook wrote in *GTE Corp.*, "it is hard to read § 2511 in that way." *Id.* at 659. § 2511(1) is very precise about who, other than primary interceptors, can be liable. "A statute that is this precise . . . should not be read to create a penumbra of additional but unspecified liability." *Id.*; *cf. Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1005 (9th Cir. 2006) (declining to expand civil liability under §§ 2702 and 2707 of the ECPA to include conspirators as well as aiders and abetters). Without any persuasive authority for expanding the Wiretap Act to include secondary liability, the Court will not do so now. If Garback chooses to re-plead his Wiretap Act claim against Shwedel, he must allege that Garback himself intercepted emails or used them with knowledge they were unlawfully intercepted.

b. Title II of the ECPA - 18 U.S.C. § 2701 ("The Stored Communications Act")

Garback also asserts a claim under Title II of the ECPA – the Stored Communications Act, 28 U.S.C. §§ 2701 *et seq*.[5] Section 2701 provides, in relevant part:

> Except as provided in subsection (c) of this section whoever-
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished . . . .

18 U.S.C. § 2701(a). A private right of action is available for any person aggrieved by an intentional or knowing violation of the statute. 18 U.S.C. § 2707(a).

Congress's general purpose of the ECPA, including the Stored Communications Act, was to create a cause of action against "'computer hackers (e.g., electronic trespassers).'" *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000) (quoting *State Wide Photocopy Corp. v. Tokai Fin. Servs., Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995)). Section 2701(a) prohibits the intentional and unauthorized *access* of an electronic communication service and subsequent obtainment, alteration, or prevention of authorized access to the service. *Id.* It does not, however, prohibit *disclosing* and otherwise *using* the information obtained therefrom. *Id.* (citing *Wesley Coll. v. Pitts*, 974 F. Supp. 375, 389 (D. Del. 1997)); *accord Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 966 (M.D. Tenn. 2008); *In re Am. Airlines, Inc., Privacy Litig.*, 370 F. Supp. 2d 552, 558-59 (N.D. Tex. 2005).

---

[5] Although the body of the complaint does not actually allege a violation of § 2701, the heading for count one does refer to the statute so the Court addresses it on the assumption that Garback intended to state a claim under § 2701.

Applying these standards, the allegations in Garback's complaint are insufficient to state a claim against Shwedel for violation of §§ 2701 and 2707. Garback has not come close to alleging that Shwedel himself accessed a facility through which an electronic communication service is provided. Rather, he alleges that defendant *Cyber-Trace* accessed his email account. Even if Shwedel used this information, however, such use is not actionable. Accordingly, Garback has failed to state a claim against Shwedel for violation of §§ 2701 and 2707.[6]

2. Count Two - Intrusion Upon Seclusion

Garback alleges in count two that Shwedel intruded upon Garback's seclusion. The tort of intrusion upon seclusion is grounded in the common-law right of privacy. *Battaglieri v. Mackinac Ctr. of Public Policy*, 261 Mich. App. 296, 300 (2004). The Michigan Court of Appeals recently reiterated the nature of the tort, and its elements:

> An action for intrusion upon seclusion focuses on the manner in which information is obtained, not its publication; it is considered analogous to a trespass. There are three necessary elements to establish a prima facie case of intrusion upon seclusion: (1) the existence of a secret and private subject matter; (2) a right possessed by the plaintiff to keep that subject matter private; and (3) the obtaining of information about that subject matter through some method objectionable to a reasonable man.

Begin v. Mich. Bell Tel. Co., 284 Mich. App. 581, 605 (2009) (quoting *Doe v. Mills*, 212 Mich. App. 73, 88 (1995)). Any attempt to plead intrusion upon seclusion based solely

[6] To the extent Garback claims that Shwedel conspired with the other defendants to access his emails, *see* Pl.'s Resp. Br., at 12, this claim fails because, just as with § 2511, Congress did not expressly provide for secondary liability for violations of §§ 2701 and 2707 and Garback offers no persuasive authority for implying such liability. *See, e.g.*, *Jones v. Global Information Group, Inc.*, No. 06-00246, 2009 WL 799745, *2 (W.D. Ky. Mar. 25, 2009) (declining to recognize liability for one who aided and abetted others or conspired with others to violate § 2701); *cf. Freeman*, 457 F.3d at 1005 (declining to expand liability under §§ 2702 and 2707 to create a private right of action for claims of conspiracy or aiding and abetting).

upon the *use* of information obtained in an objectionable manner fails to state a claim. *See Mills*, 212 Mich. App. at 89.

Shwedel contends that the intrusion claim against him fails because the complaint alleges only that Shwedel *used* private information about Garback that was obtained by the other defendants in an objectionable manner. The complaint goes further, however, and alleges that Shwedel conspired and acted in concert with the other defendants to intrude upon Garback's seclusion. Compl. ¶¶ 12, 32-39. "'Conspiracy, by reason of the connection it involves among the conspirators, may cause individuals to be responsible, who, but for the conspiracy, would not be responsible at all.'" *Roche v. Blair*, 305 Mich. 608, 614 (1943) (quoting *Bush v. Sprague*, 51 Mich. 41, 48 (1883)). Because, as far as the Court can tell, Garback has stated a valid claim against the defendants who directly committed the underlying tort, liability may run to Shwedel if he conspired with the other defendants to commit the tort.

The problem, however, is that the complaint contains only legal conclusions, while lacking well-pleaded allegations with respect to conspiracy. At paragraph 12, for example, Garback alleges in conclusory fashion that "Lossing had conspired with the other defendants for the purpose of intercepting Garback's emails . . . and [used] those stolen communications as a basis for negotiations in the divorce." Compl. ¶ 12. Furthermore, the few factual allegations that do appear in the complaint do not support the claim that Shwedel conspired with any of the other defendants. Rather, Garback alleges that Lossing hired Cyber-Tech to hack into Garback's email. Once Lossing received the emails, she forwarded the information in the emails to Shwedel. Compl. ¶ 17. There are no allegations supporting a meeting of the minds among the defendants to accomplish this tort. These allegations fail to suggest a plausible claim of civil conspiracy on the part of Shwedel.

3. Count Three - Intentional Infliction of Emotional Distress

Garback also asserts a claim against Shwedel for intentional infliction of emotional distress ("IIED"). To state a claim for IIED, the plaintiff must plead: 1) extreme and outrageous conduct; 2) intent or recklessness; 3) causation; and 4) severe emotional distress. *Roberts v. Auto-Owners Ins., Co.*, 422 Mich. 594, 602 (1985).[7] Liability attaches only when a plaintiff can demonstrate that the defendant's conduct is "so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious and utterly intolerable in a civilized community." *Id.* at 602-03 (quoting Restatement (Second) of Torts, § 46, cmt. d, at 72-73).

The Court finds that the allegations in the complaint do not state a plausible claim against Shwedel for IIED. The deficiencies lie primarily with the intent and injury elements of the tort. Although Garback has alleged the elements of the cause of action, this is not enough to state a claim. *Iqbal*, 129 S. Ct. at 1949 ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice."). Garback's incorporation of the other allegations in the complaint also do not demonstrate a plausible claim against Shwedel. The complaint alleges only that Shwedel used the unlawfully retrieved information to craft negotiating strategies in the divorce. The allegations with respect to intent are insufficient. A plaintiff may satisfy the intent element of the tort in two ways: 1) showing that a defendant specifically intended to cause a plaintiff emotional distress; or 2) showing that defendant's conduct was so reckless that any reasonable person would know emotional distress would result. *Lewis v. LeGrow*, 258 Mich. App. 175, 198 (2003). The factual allegations fail to demonstrate intent or recklessness.

[7] The Michigan Supreme Court has never officially recognized a cause of action for IIED, but has implied that it would do so if presented with the right facts. *See Roberts*, 422 Mich. at 611.

Garback has also failed to sufficiently plead the fourth element of the tort: severe emotional distress. "'The law intervenes only where the distress inflicted is so severe that no reasonable man could be expected to endure it.'" *Roberts*, 422 Mich. at 608-09 (quoting Restatement (Second) of Torts, § 46, cmt. j, at 77)). Anger is insufficient by itself to demonstrate actionable emotional distress. *Id.* at 610. Garback alleges in a conclusory fashion that he "suffer[ed] severe emotional distress." Compl. ¶ 26. But, there are no factual allegations supporting this conclusion. There are no allegations that Garback suffered grief, depression, disruption of lifestyle, or that he required treatment for anxiety or depression. These types of allegations are necessary to state a claim of IIED *See id.* at 611. This absence of detail is fatal to his claim of IIED.

4. Count Four - Violation of Michigan Unauthorized Access to Computers Statutes

In Count Four Garback alleges Shwedel violated various sections of the Michigan code relating to unauthorized access to computers, Mich. Comp. Laws §§ 752.791-797. Shwedel argues that these statutes are penal in nature and do not provide a private right of action. The statutory provisions referenced in Garback's complaint fall under Chapter 752 of the Michigan's Compiled Laws entitled "Crimes and Offenses." Garback offers no authority, and the Court has found none, allowing the Court to permit enforcement of the criminal statute through a private civil action. In Michigan, the rule is that if a right to relief is provided by statute, there is no private cause of action for enforcement unless the statute expressly creates one, or one can be inferred from the fact that the statute provides no adequate means of enforcement. *See Long v. Chelsea Cmty. Hosp.*, 219 Mich. App. 578, 583 (1996). Neither prong is satisfied here. *See* Mich. Comp. Laws § 752.797 (discussing enforcement); *cf. Marx v. Centran Corp.*, 747 F.2d 1536, 1549 (6th Cir. 1984) ("[W]here there is a 'bare criminal statute, with absolutely no indication that civil enforcement of any

kind was available to anyone,' a private cause of action will not be inferred." quoting *Cort v. Ash*, 422 U.S. 66, 80 (1975)).

Garback did not respond to the motion's attack on this count. For this reason, the count will be dismissed with prejudice. Garback may not re-plead this count in an amended complaint.

5. Count Seven - Punitive Damages[8]

Garback asserts a claim for punitive damages. "Punitive damages are available in Michigan *only* when expressly authorized by the Legislature." *Gilbert v. Daimler Chrysler Corp.*, 470 Mich. 749, 765 (2004) (emphasis in original). Garback provides no statutory authority in his complaint or his response brief – indeed, he failed even to address the motion's challenge of this count – that support the recovery of punitive damages on any of the claims asserted in the complaint. The claim for punitive damages will be dismissed with prejudice. Garback may not re-plead this count in an amended complaint.

CONCLUSION

Garback has failed to state a claim against Shwedel. The Court will grant Shwedel's motion to dismiss. The Court will grant Garback leave to file an amended complaint. Leave is not granted, however, on the claims for violation of Mich. Comp. Laws § 752.794 and the claim for punitive damages, nor will claims likely survive if asserted against all defendants in a blanket manner. Failure to address the deficiencies will result in dismissal of the claims against Shwedel with prejudice.

WHEREFORE it is hereby **ORDERED** that defendant Shwedel's motion to dismiss the claims against him (docket no. 5) is **GRANTED.**

---

[8] Because of the presence of two counts labeled "V," "Count VI" is in fact the seventh count alleged in the complaint.

IT IS FURTHER ORDERED that Plaintiff shall have 21 days to file an amended complaint, consistent with Rule 11, that remedies the deficiencies identified above.

SO ORDERED.

s/Stephen J. Murphy, III
STEPHEN J. MURPHY, III
United States District Judge

Dated: September 20, 2010

I hereby certify that a copy of the foregoing document was served upon the parties and/or counsel of record on September 20, 2010, by electronic and/or ordinary mail.

Alissa Greer
Case Manager